EXHIBIT 4

Endpoint Verification overview

This document describes the basic concepts of Endpoint Verification.

Endpoint Verification lets security administrators or security operations professionals secure Google Cloud, on-premises apps and resources, and Google Workspace apps.

Endpoint Verification is part of Google Cloud Chrome Enterprise Premium (/beyondcorp-enterprise/docs/overview) and is available to all Google Cloud, Cloud Identity, Google Workspace for Business, and Google Workspace for Enterprise customers.

When to use Endpoint Verification

Use Endpoint Verification when you want an overview of the security posture of the devices that are used to access your organization's resources, such as laptops and desktops.

As a security administrator or security operations professional, your goal is to manage secure access to your organization's resources. The employees of your organization can use either the company-owned devices or their unmanaged personal devices to access the organization's resources. When Endpoint Verification is installed on the devices that access your organization's resources, it collects and reports device inventory information. You can use this device inventory information to manage secure access to your organization's resources.

When paired with the other offerings of Chrome Enterprise Premium, Endpoint Verification helps enforce fine-grained access control on your Google Cloud resources.

How Endpoint Verification works

Endpoint Verification consists of a Chrome extension that collects and reports device inventory information by constantly syncing with Google Cloud. Endpoint Verification creates an inventory of devices with Chrome browser that access your organization's data.

For example, after Endpoint Verification is deployed on devices that are used to access Google Cloud resources, Endpoint Verification populates information about those devices. As an administrator, you can review the device information including encryption status, OS, and other details, and use this information to manage access control.

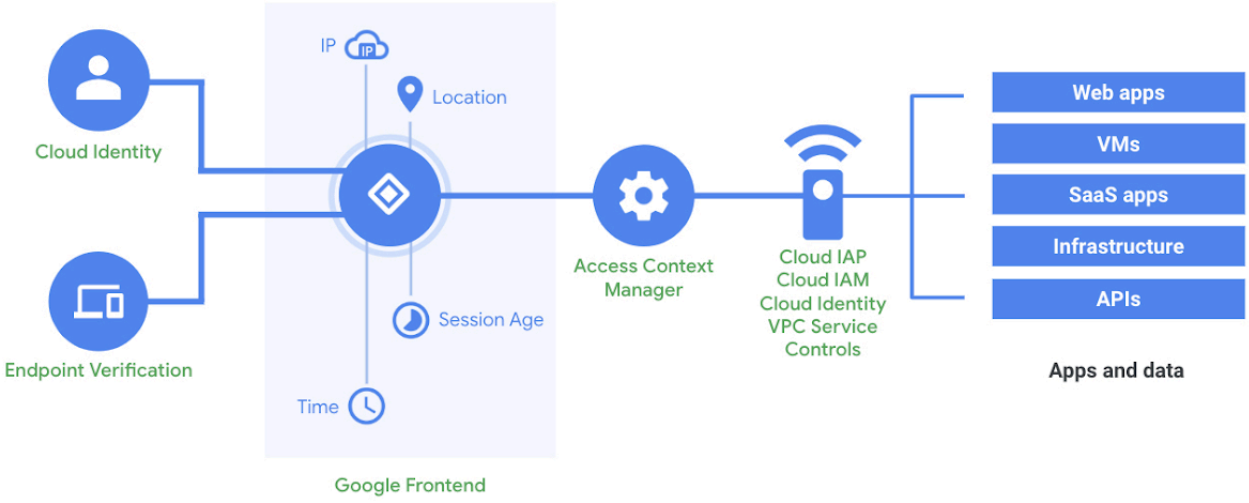
For more information, see Device attributes collected by Endpoint Verification (/endpoint-verification/docs/device-information).

How Endpoint Verification works with Access Context Manager

Access Context Manager (/access-context-manager/docs), which is part of Google Cloud Chrome Enterprise Premium (/beyondcorp-enterprise/docs/overview), lets security administrators or security operations professionals define fine-grained and attribute-based access control for projects and resources in Google Cloud and resources in Google Workspace.

Access Context Manager references the device attributes collected by Endpoint Verification to enforce fine-grained access control with access levels (/access-context-manager/docs/overview#access-levels).

The following diagram shows how Endpoint Verification works with Access Context Manager:

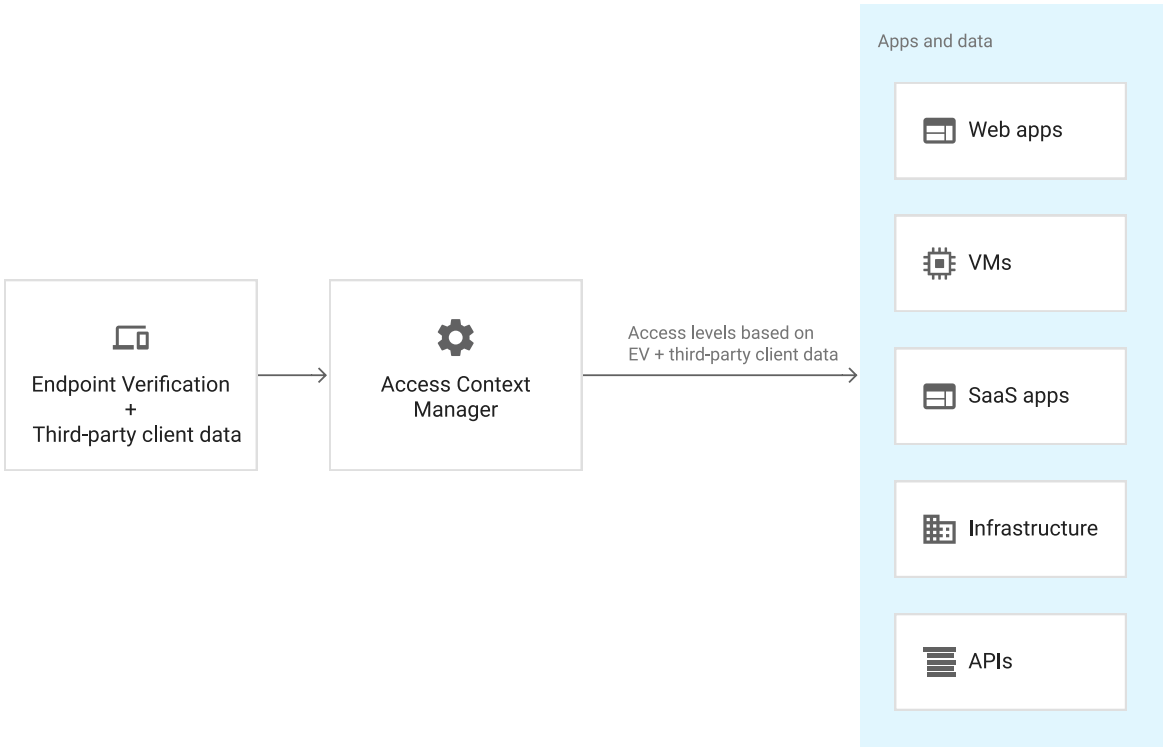


How Endpoint Verification works with third-party clients

In Chrome Enterprise Premium and third-party client integrations (/beyondcorp-enterprise/docs/integration-docs), third-party clients such as CrowdStrike and Microsoft Intune collect real-time device information. Endpoint Verification communicates with these third-party clients to collect their device information and makes them available for Access Context Manager (/access-context-manager/docs).

Access Context Manager references the device attributes collected by Endpoint Verification and third-party clients to enforce fine-grained access control with access levels (/access-context-manager/docs/overview#access-levels).

The following diagram shows how Endpoint Verification and third-party clients work with Access Context Manager:



What's next

- Quickstart: Set up Endpoint Verification on your devices (/endpoint-verification/docs/quickstart)
- Device attributes collected by Endpoint Verification (/endpoint-verification/docs/device-information)
- Deploy Endpoint Verification (/endpoint-verification/docs/deploying-with-admin-console)

Last updated 2025-01-30 UTC.